REMARKS

I. Introduction

In response to the Office Action dated May 7, 2008, claims 1 and 16 have been amended. Claims 1-30 remain in the application. Re-examination and re-consideration of the application is requested.

II. Claim Amendments

Applicants' attorney has made amendments to the claims as indicated above. These amendments were made solely for the purpose of clarifying the language of the claims, and were not required for patentability or to distinguish the claims over the prior art.

III. Prior Art Rejections

A. The Office Action Rejections

In paragraphs (4)-(5) of the Office Action, claims 1-7, 10-22, and 25-30 were rejected under 35 U.S.C. §103(a) as being unpatentable over Denning et al., U.S. Patent No. 7,143,289 (Denning) in view of Brundage et al., U.S. Patent No. 7,249,257 (Brundage). In paragtaph (19) of the Office Action, claims 8-9 and 23-24 were rejected under 35 U.S.C. §103(a) as being unpatentable over Denning in view of Brundage and further in view of Clapper, U.S. Publication No. 2003/0108202 (Clapper).

Applicants' attorney respectfully traverses these rejections.

B. The Applicants' Independent Claims

Independent claims 1 and 16 are generally directed to data set comparison and net change processing by a computer. Independent claim 1 is representative and recites a method for identification, processing, and comparison of location coordinate data in a confidential and anonymous manner, comprising: receiving a plurality of fixed coordinates, each of the fixed coordinates independently representing a location of an item; utilizing a cryptographic algorithm to encrypt the plurality of fixed coordinates, thereby forming a processed data; and comparing the processed data to at least a portion of secondary data that comprises one or more fixed coordinates to determine whether a match exists between the encrypted fixed coordinates of the processed data and the fixed coordinates of the secondary data.

C. The Denning Reference

Denning describes a system and method for delivering encrypted information in a communication network using location identity and key tables, wherein access to digital data is controlled by encrypting the data in such a manner that, in a single digital data acquisition step, it can be decrypted only at a specified location, within a specific time frame, and with a secret key. Data encrypted in such a manner is said to be geo-encrypted. This geo-encryption process comprises a method in which plaintext data is first encrypted using a data encrypting key that is generated at the time of encryption. The data encrypting key is then encrypted (or locked) using a key encrypting key and information derived from the location of the intended receiver. The encrypted data encrypting key is then transmitted to the receiver along with the ciphertext data. The receiver both must be at the correct location and must have a copy of the corresponding key decrypting key in order to derive the location information and decrypt the data encrypting key. After the data encrypting key is decrypted (or unlocked), it is used to decrypt the ciphertext. If an attempt is made to decrypt the data encrypting key at an incorrect location or using an incorrect secret key, the decryption will fail. If the sender so elects, access to digital data also can be controlled by encrypting it in such a manner that it must traverse a specific route from the sender to the recipient in order to enable decryption of the data. Key management can be handled using either private-key or public-key cryptography. If private-key cryptography is used, the sender can manage the secret key decrypting keys required for decryption in a secure manner that is transparent to the recipient. As a consequence of its ability to manipulate the secret keys, the sender of encrypted data retains the ability to control access to its plaintext even after its initial transmission.

D. The Brundage Reference

Brundage describes maps and signs embedded with plural-bit data in the form of digital watermarks. In one embodiment, the plural-bit data includes location information with respect to a map. A handheld reading device extracts the location information from the map. The reading device then compares the location information with a physical location of the device. Feedback is provided to help a device user to correlate the map location with the physical location. In another embodiment, signs are watermarked to provide navigational and informational aids. The watermarks may include unique identifiers, which allow database lookup of related information.

E. The Clapper Reference

Clapper describes location dependent encryption and/or decryption, wherein encryption and decryption may be tied to physical location information, e.g., GPS or other position data. Decryption keys may be defined with respect to a location at which decryption is to occur. A clock may be used to ensure decryption is occurring at a desired decryption location. For security, names may be associated with GPS position data, where encrypted data and a name associated with position data may be provided to a recipient, and the recipient is required to know or have access to the position data associated with the name in order to compute a decryption key. For additional security, encryption may also be performed with respect to position data for an encryption location, where an identifier associated with the encryption location is provided to the recipient, and the recipient is required to know or have access to the position data associated with the second name. Other embodiments are disclosed.

F. The Applicants' Invention is Patentable Over the References

The Applicants' claimed invention is patentable over the references, because the claims contain limitations not taught by the reference. Specifically, Applicants' invention is designed to use a cryptographic algorithm to identify, disclose and compare multiple sets of coordinates representing the location of a particular item in a secure and confidential manner. These essential features are not taught or suggested by the references.

The Office Action, on the other hand, asserts that Denning shows the elements of the independent claims directed to "receiving a plurality of fixed coordinates, each independently representing a location of an item," at the following locations:

Denning: Fig. 3

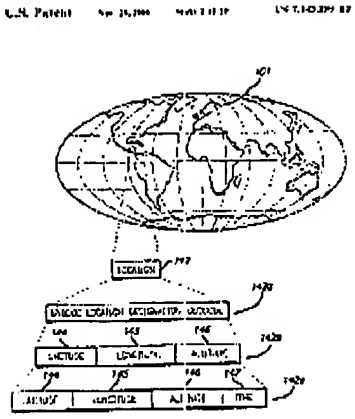

FIG. 3

Denning: Fig. 6

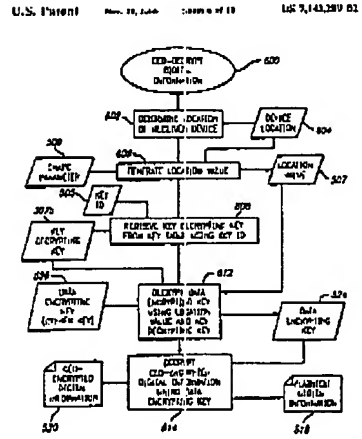

FIG. 6

Denning: col. 3, lines 23-27

Data encrypted in such a manner is said to be geo-encrypted. This geo-encryption process comprises a method in which plaintext data is first encrypted using a random data encryption key that is generated at the time of encryption. **The data encrypting key is then encrypted (or locked) using a location value and a key encrypting key. The encrypted data encrypting key is then transmitted to the receiver along with the ciphertext data.** The receiver both must be at the correct location and must have a copy of a corresponding key decrypting key in order to derive the location key and decrypt the data encrypting key. After the data

> encrypting key is decrypted (or unlocked), it is used to decrypt the ciphertext. If an attempt is made to decrypt the data encrypting key at an incorrect location or using an incorrect key decryption key, the decryption will fail. In addition, the encrypted data encrypting key or ciphertext optionally may be rendered unusable so that it becomes impossible to ever decrypt that particular ciphertext. The data encrypting key may also be encrypted in a manner that it can only be accessed at a certain time or during a specific time frame.

Applicants' attorney disagrees.

The above portions of Denning merely describe a single location value, not a plurality of fixed coordinates, wherein each of the fixed coordinates independently represent a location of an item, as recited in Applicants' claims. The fact that Denning's single location value in Fig. 3 is comprised of multiple values, namely latitude, longitude, altitude and time, is irrelevant. Applicants' claim limitations require that each of the fixed coordinates independently represent a location of an item, which is not met by Denning's single location value comprised of latitude, longitude, altitude and time. In other words, Applicants' claim limitations would be read on only by a plurality of independent location values in Denning, wherein each of independent location values represent the location of an item.

In addition, the Office Action asserts that Denning shows the elements of the independent claims directed to "utilizing a cryptographic algorithm to encrypt the plurality of fixed coordinates, thereby forming a processed data," at the following locations:

Denning: Fig. 5

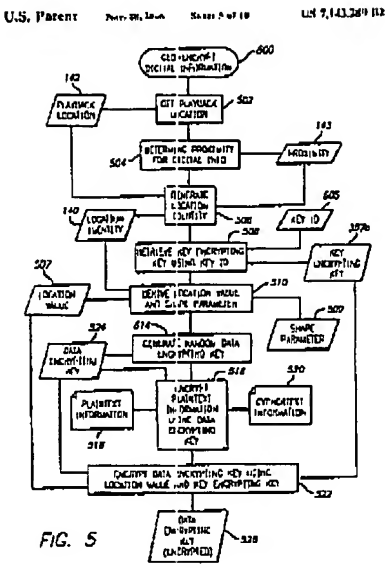

FIG. 5

Denning: Fig. 6

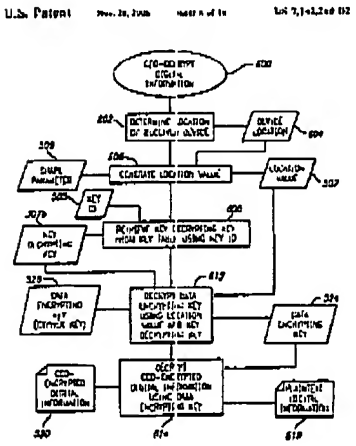

FIG. 6

Denning: col. 6, lines 17-21

Associating Location Identity. A method of marking digital data encryption keys with a location identity attribute.

Applicants' attorney disagrees.

Applicants' attorney notes that the full limitation recites "utilizing a cryptographic algorithm to encrypt the plurality of fixed coordinates, thereby forming a processed data," not "utilizing a cryptographic algorithm to ~~encrypt~~ process the plurality of fixed coordinates ~~, thereby~~ forming a processed data," as asserted by the Office Action.

This is an important distinction, because the above portions of Denning merely describe how digital data encryption keys are marked with a location identity attribute. However, the above portions of Denning do not teach or suggest utilizing a cryptographic algorithm to encrypt the location identity attribute.

The Office Action also asserts that Denning shows the elements of the independent claims directed to "comparing the processed data to at least a portion of secondary data that comprises one or more fixed coordinates to determine whether a match exists between the encrypted fixed coordinates of the processed data and the fixed coordinates of the secondary data," at the following locations:

Denning: Fig. 6

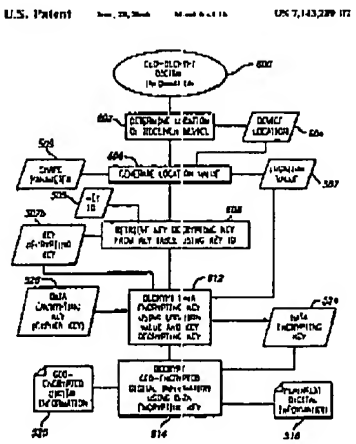

FIG. 6

Denning: col. 12, lines 39-48

Then, at step 514, the process generates a random data encrypting key 524. This data encrypting key 524 is used to encrypt the plaintext digital information 518 at step 516 to produce geo-encrypted digital information 520. The data encrypting key 524 is then encrypted at step 522 using the location value 507 and the key encrypting key 307a. **The geo-encrypted digital information 520, the encrypted data encrypting key 526 (also referred to below as a cipher key), the shape parameter 509, and the key ID 505 are then communicated to the receiver**

device 400. Attempts to decrypt the geo-encrypted information 520 by a receiver device 400 will be denied unless the location of the receiver device 400 matches the location specified by the location identity attribute 140 and the receiver device 400 has the correct key decrypting key identified by the key ID 505.

Denning: col. 16, lines 29-33

The Geo-Decrypt function 720 has five inputs, including: (1) Shape Parm 509; (2) Key ID 505; (3) Cipher Key 526; (4) IV 708; and (5) Ciphertext 520. The Geo-Decrypt function 720 decrypts Ciphertext 520 using Data Encrypting Key 524 and IV 708, and includes sub-function Decrypt 724 and accesses the Geo-Unlock Key function 820 (described below with respect to FIG. 8). Data Encrypting Key 524 is determined by unlocking the Cipher Key using the Geo-Unlock Key function 820. **The Geo-Unlock Key function 820 decrypts the Cipher Key 526 using the key decrypting key identified by Key ID and a location value determined from the Shape Parm 509 and a GPS signal 727 in order to yield the Data Encrypting Key 524.** The Decrypt sub-function 724 decrypts the Ciphertext 520 using the Data Encrypting Key 524 and IV 708 in order to reconstruct the Plaintext 518. It should be appreciated that the Decrypt sub-function 724 would be the inverse of the Encrypt sub-function 706 used by the Geo-Encrypt function 700 described above.

Applicants' attorney disagrees.

Denning merely describes geo-encrypting data, i.e., encrypting data using a random data encryption key, encrypting or locking the random data encrypting key using a location value and a key encrypting key, and then transmitting the encrypted random data encrypting key to a receiver along with the data encrypted by the random data encryption key. However, nowhere do the above portions of Denning describe the encrypted data as being location coordinate data, and nowhere do the above portions of Denning describe a comparison being performed on the encrypted location coordinate data.

Finally, the Office Action admits that Denning does not explicitly teach "between the encrypted fixed coordinates of the processed data and the fixed coordinates of the secondary data." Nonetheless, the Office Action asserts that Brundage shows these elements of the independent claims at the following locations:

Brundage: Fig. 4

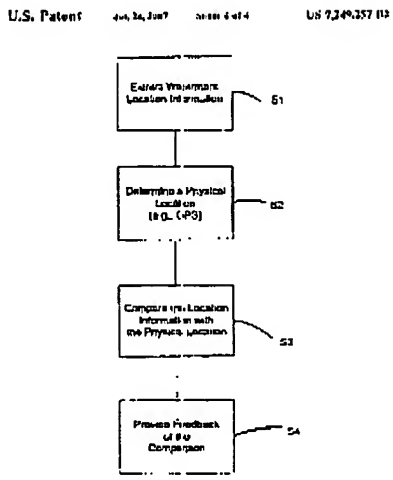

FIG. 4

Brundage: col. 4, lines 28-41

A watermark typically includes a payload (e.g., 16 256 bits) that provides area (or location) identifying information. For example, the payload may include the geo-coordinates (e.g., "center lat: N34.4324352, long: W87.2883134; rot from N/S: 3.232;x2.343, y2.340, dx0.123, dy493, etc.") for the center of the area, the coordinates of each area corner or boundary, the area of the boundary, a range of coordinates for the area, coordinates in relation to the overall area depicted by the map, and/or the coordinates for a dominate (or well-known) structure, road, area, etc., within the area block. (For example, area A is embedded with at least one watermark having coordinates corresponding to area A's center or corners, etc.). The payload may simply be a number that is associated with a block location on the map. For example, if a map comprises 32 by 64 watermarked blocks, each block is encoded with a number between 1 and 2048.

Brundage: col. 4, line 67 – col. 5, line 24

As an alternative, the location information may include an index or identifier, which is used to interrogate a database to find physical coordinates or location information. Upon extraction by a watermark decoder, the index is provided to a database. The decoder may communicate with a database via a network (e.g., wireless network, LAN, WAN, the internet, intranet, etc.). Alternatively, the database may be maintained locally, or stored on a computer readable medium such as a compact disk (CD), magnetic tape, magnetic storage device (disk drive, removable media, floppy disks, etc.), electronic memory circuits, etc. Related information that is stored in the database is indexed via the watermark index.

> A grid (or orientation) signal can also be included in the watermark and/or location information. Preferably, the entire map uses the same grid signal, so that all blocks in a map can be used to determined rotation and scale of the map. Such a grid signal may assist in detecting watermarks. (Alternatively, such a grid signal can be used to help orient a map. For example, an orientation signal may be used to designate magnetic North, or another map orientation. Feedback can be supplied to a reader (e.g., watermark decoder) to help orient a watermark reader with respect to a map and the physical surrounding area. As discussed below, a watermark reader may be provided with compass-like functionality to assist with such orientation.).
>
> Brundage: col. 7, lines 51-56
>
> **In another embodiment, the watermark's encoded data includes identification of a map's grid system.** The reading device 20 correlates (e.g., via formula or table/database look-up) the grid system to the GPS coordinate system and conveys to a user her current map grid location (e.g., tells her that she is currently located in grid F-9).

Applicants' attorney disagrees.

Brundage merely describes maps and signs embedded with plural-bit data in the form of digital watermarks, wherein the plural-bit data includes location information with respect to a map. In Brundage, a handheld reading device extracts the location information from the map and the reading device then compares the location information with a physical location of the device.

However, the location information in Brundage is merely encoded into watermarks, not encrypted. Moreover, the location information in Brundage is used only after it has been decoded from the watermarks, it is never used in encoded or encrypted form; instead, it is only stored in encoded form. Further, the location information in Brundage is never compared with other location information in encoded or encrypted form, e.g., while encoded within the watermark. Consequently, the above portions of Brundage do not teach or suggest determining whether a match exists between encrypted fixed coordinates of processed data and fixed coordinates of secondary data, in the context of there being a plurality of fixed coordinates, each of the fixed coordinates independently representing a location of an item, the plurality of fixed coordinates being encrypted to form processed data, and the encrypted fixed coordinates of the processed data being compared to the fixed coordinates of the secondary data.

Thus, the combination of Denning and Brundage does not teach or suggest the limitations of Applicants' independent claims. Indeed, neither Denning nor Brundage operate in the same context as Applicants' claims, namely using a cryptographic algorithm to identify, process and compare multiple sets of coordinates, wherein each set of coordinates independently represents the location of a particular item, in a secure and confidential manner.

Moreover, the Clapper reference does not overcome the deficiencies of the Denning reference. Recall that Clapper was cited only against dependent claims 8-9 and 23-24 and only for disclosing a uniform and non-uniform grid, in the context of overlaying a residential area.

Thus, Applicants' attorney submits that independent claims 1 and 16 are allowable over Denning, Brundage, and Clapper. Further, dependent claims 2-15 and 17-30 are submitted to be allowable over Denning, Brundage, and Clapper in the same manner, because they are dependent on independent claims 1, and 16, respectively, and thus contain all the limitations of the independent claims. In addition, dependent claims 2-15 and 17-30 recite additional novel elements not shown by Denning, Brundage, and Clapper.

IV. Conclusion

In view of the above, it is submitted that this application is now in good order for allowance and such allowance is respectfully solicited.

Should the Examiner believe minor matters still remain that can be resolved in a telephone interview, the Examiner is urged to call Applicants' undersigned attorney.

Respectfully submitted,

GATES & COOPER LLP
Attorneys for Applicants

Howard Hughes Center
6701 Center Drive West, Suite 1050
Los Angeles, California 90045
(310) 641-8797

Date: August 7, 2008

By: _____
Name: George H. Gates
Reg. No.: 33,500

GHG/kay

G&C 30571.303-US-U1